App. No. 10/734,846
Filing Date: 12/12/2003

Docket JP920030198US1

IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A method of generating a password for at least one application using a single key, said method comprising the steps of:

receiving said single key by a password generator;

receiving a first application name by the password generator at a first time, wherein the first application name is associated with a first application; ~~and~~

generating a first instance of a first password for said first application by the password generator, wherein the generating of the first instance of the first password is, based on at least ~~said single key~~ and said first application name received at the first time and based on said single key;

receiving said first application name again by the password generator at a second time; and

generating a second instance of the first password for said first application by the password generator, wherein the generating of the second instance of the first password is based on at least said first application name received at the second time and based on said single key, and the generated first password is identical in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the first and second times.

2. (currently amended) The method according to claim 1, comprising the further steps of:

receiving a second application name by the password generator at a third time, wherein the second application name is different than the first application name and is associated with a second application; ~~and~~

generating a first instance of a second password for said second application by the password generator, wherein the generating of the first instance of the second password is, based on ~~said single key~~ and said second application name received at the third time and based on said single key, wherein the second password is different than the first password;

receiving said second application name again at a fourth time by the password generator; and

generating a second instance of the second password for said second application by the password generator, wherein the generating of the second instance of the second password is based on at least said second application name received at the fourth time and based on said single key and the generated second password is identical in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the third and fourth times.

3. (currently amended) The method according to claim 1, comprising the further step of:

receiving a user specified time interval by the password generator indicating an interval during which the password generator is to produce identical instances of the first password for identical instances of the received first application name and single key; and

generating a third instance of the first password responsive to receiving said application name at a time after expiration of the interval, wherein in the third instance the generated first password is different than the first and second instances of the first password, even though the application name received for generating the third instance of the first password is identical to the application name received at the first and second times.

~~time period;~~

~~wherein generating said first password is further based on said time period.~~

4. (original) The method according to claim 1, comprising the further step of:

receiving first password constraints for said first password;

wherein generating said first password is further based on said first password constraints.

5. (original) The method according to claim 1, wherein generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

6. (original) The method according to claim 1, comprising the further step of:

generating a first userid for said first application, based on at least said single key and said first application name.

7. (original) The method according to claim 6, comprising the further step of:

receiving a first userid time period;

wherein generating said first userid is further based on said first userid time period.

8. (original) The method according to claim 6, comprising the further step of:

receiving first userid constraints for said first userid;

wherein generating said first password is further based on said first userid constraints.

9. (original) The method according to claim 6, wherein generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

10. (original) The method according to claim 1, wherein said first application is selected from the group of applications consisting of bank account, Internet email account, Internet website, and computer account.

11-17. (canceled)

18. (currently amended) A computer system comprising:

a processor; and

a storage device connected to the processor, wherein the storage device has stored thereon a password generation program for controlling the processor, and wherein the processor is operative with the program to execute the program for performing the steps of:

~~An apparatus for generating a password for at least one application using a single key, said apparatus comprising:~~

~~means for~~ receiving ~~a said~~ single key by a password generator;

~~means for~~ receiving a first application name by the password generator at a first time, wherein the first application name is associated with a first application; ~~and~~

~~means for~~ generating a first instance of a first password for said first application by the password generator, wherein the generating of the first instance of the first password is~~,~~ based on at least ~~said single key~~ and said first application name received at the first time and based on said single key;

receiving said first application name again by the password generator at a second time; and

generating a second instance of the first password for said first application by the password generator, wherein the generating of the second instance of the first password is based on at least said first application name received at the second time and based on said single key, and the generated first password is identical in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the first and second times.

19. (currently amended) The ~~apparatus according to~~computer system of claim 18, wherein the steps further compris~~ing~~:

~~means for~~ receiving a second application name by the password generator at a third time, wherein the second application name is different than the first application name and is associated with a second application; ~~and~~

~~means for~~ generating a first instance of a second password for said second application by the password generator, wherein the generating of the first instance of the second password is~~,~~ based on ~~said single key~~ and said second application name received at the third time and based on said single key, wherein the second password is different than the first password;

receiving said second application name again at a fourth time by the password generator; and

generating a second instance of the second password for said second application by the password generator, wherein the generating of the second instance of the second password is based on at least said second application name received at the fourth time and based on said single key and the generated second password is identical in its first and second instances, if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the third and fourth times.

20. (currently amended) The ~~apparatus according to~~computer system of claim 18, wherein the steps further compris~~e~~ing:

~~means for~~ receiving a user specified time interval by the password generator indicating an interval during which the password generator is to produce identical instances of the first password for identical instances of the received first application name and single key; and

generating a third instance of the first password responsive to receiving said application name at a time after expiration of the interval, wherein in the third instance the generated first password is different than the first and second instances of the first password, even though the application name received for generating the third instance of the first password is identical to the application name received at the first and second times.

~~time period;~~

~~wherein said means for generating said first password utilises said time period.~~

21. (currently amended) The ~~apparatus according to~~computer system of claim 18, wherein the steps further compris~~e~~ing:

~~means for~~ receiving first password constraints for said first password;

wherein ~~said means for~~ generating said first password utilises said first password constraints.

22. (currently amended) The ~~apparatus according to~~computer system of claim 18, wherein ~~said means for~~ generating said first password utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data

Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

23. (currently amended) The ~~apparatus according to~~computer system of claim 18, wherein the steps further compris~~e~~ing:

~~means for~~ generating a first userid for said first application, based on at least said single key and said first application name.

24. (currently amended) The ~~apparatus according to~~computer system of claim 23, wherein the steps further compris~~e~~ing:

~~means for~~ receiving a first userid time period;

wherein ~~said means for~~ generating said first userid utilises said first userid time period.

25. (currently amended) The ~~apparatus according to~~computer system of claim 23, wherein the steps further compris~~e~~ing:

~~means for~~ receiving first userid constraints for said first userid;

wherein ~~said means for~~ generating said first password utilises said first userid constraints.

26. (currently amended) The ~~apparatus according to~~computer system of claim 23, wherein ~~said means for~~ generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

27. (currently amended) A computer program product comprising a storage medium readable by a computer ~~readable medium~~ having a computer program recorded therein for generating a password for at least one application using a single key, said computer program comprising:

computer program code means for receiving said single key by a password generator;

computer program code means for receiving a first application name by the password generator at a first time, wherein the first application name is associated with a first application; ~~and~~

computer program code means for generating a first instance of a first password for said first application by the password generator, wherein the generating of the first instance of the first password is~~,~~ based on at least ~~said single key~~ and said first application name received at the first time and based on said single key;

receiving said first application name again by the password generator at a second time; and

generating a second instance of the first password for said first application by the password generator, wherein the generating of the second instance of the first password is based on at least said first application name received at the second time and based on said single key and the generated first password is identical in its first and second instances, and the second time is at least 24 hours after the first time, if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the first and second times.

28. (currently amended) The computer program product according to claim 27, further comprising:

computer program code means for receiving a second application name by the password generator at a third time, wherein the second application name is different than the first application name and is associated with a second application; ~~and~~

computer program code means for generating a first instance of a second password for said second application by the password generator, wherein the generating of the first instance of the second password is~~,~~ based on ~~said single key~~ and said second application name received at the third time and based on said single key, wherein the second password is different than the first password;

receiving said second application name again at a fourth time by the password generator; and

generating a second instance of the second password for said second application by the password generator, wherein the generating of the second instance of the second password is based on at least said second application name received at the fourth time and based on said single key and the generated second password is identical in its first and second instances if no time interval has been user specified for the first and second instances or if a time interval has been user specified but has not elapsed between the third and fourth times.

29. (currently amended) The computer program product according to claim 27, further comprising:

computer program code means for receiving a user specified time interval by the password generator indicating an interval during which the password generator is to produce identical instances of the first password for identical instances of the received first application name and single key; and

generating a third instance of the first password responsive to receiving said application name at a time after expiration of the interval, wherein in the third instance the generated first password is different than the first and second instances of the first password, even though the application name received for generating the third instance of the first password is identical to the application name received at the first and second times.

~~time period;~~

~~wherein said computer program code means for generating said first password utilises said time period.~~

30. (original) The computer program product according to claim 27, further comprising:

computer program code means for receiving first password constraints for said first password;

wherein said computer program code means for generating said first password utilises said first password constraints.

31. (original) The computer program product according to claim 27, wherein said computer program code means for generating said first password utilises at least one encryption

technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.

32. (original) The computer program product according to claim 27, further comprising:

computer program code means for generating a first userid for said first application, based on at least said single key and said first application name.

33. (original) The computer program product according to claim 32, further comprising:

computer program code means for receiving a first userid time period;

wherein said computer program code means for generating said first userid utilises said first userid time period.

34. (original) The computer program product according to claim 32, further comprising:

computer program code means for receiving first userid constraints for said first userid;

wherein said computer program code means for generating said first password utilises said first userid constraints.

35. (original) The computer program product according to claim 32, wherein said computer program code means for generating said first userid utilises at least one encryption technique selected from the group of encryption techniques consisting of Block Addition, International Data Encryption Algorithm (IDEA), BLOWFISH, Software-optimized Encryption Algorithm (SEAL), RC4, Data Encryption Standard (DES), and RSA.